

## Claims

## 1. An information recording apparatus comprising:

inputting means for inputting contents information;

management information creating means for extracting the access positions for said contents information inputted and for creating management information showing one or more access positions for said contents information; and

writing means for writing said contents information inputted and said management information on a recording medium.

2. The information recording apparatus according to claim 1 wherein said management information shows the access positions for the contents information by means of time information of such contents information and addresses on the recording medium.

3. The information recording apparatus according to claim 2 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems, and wherein

said management information shows the access positions for said contents information by means of the time stamps for said transport streams and addresses on the recording medium.

4. The information recording apparatus according to claim 1 wherein, as access positions described in the management information, positions where random accesses are possible to said contents information are extracted.

5. The information recording apparatus according to claim 4 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

6. An information reproducing apparatus comprising;

reading means for reading contents information and management information from a recording medium in which said contents information and said management information showing one or more access positions for said contents information are recorded; and

reading position controlling means for controlling the reading positions of said contents information on said recording medium based on said management information read from said recording medium.

7. The information reproducing apparatus according to claim 6 wherein said management information shows the access positions for the contents information by means of time information of the contents information and addresses on the recording medium.

8. The information reproducing apparatus according to claim 7 wherein said contents information is recorded on the recording medium in the form of transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents

information by means of the time stamps of said transport stream and addresses on the recording medium.

9. The information reproducing apparatus according to claim 6 wherein, as access positions described in said management information, positions where random accesses to said contents information are available are shown.

10. The information reproducing apparatus according to claim 9 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

as access positions described in said management information, transport packets each containing a sequence header code are shown.

11. An information recording/reproducing apparatus comprising:

inputting means for inputting contents information;

management information creating means for extracting access positions for said contents information inputted and for creating management information showing one or more access positions for said contents information;

recording means for recording said contents information inputted and said management information on a recording medium;

reading means for reading said contents information and said management information from said recording medium; and

reading position controlling means for controlling the reading positions of said contents information on said recording medium based on said management

information read from said recording medium.

12. The information recording/reproducing apparatus according to claim 11 wherein said management information shows the access positions for contents information by means of the time information of the contents information and addresses on the recording medium.

13. The information recording/reproducing apparatus according to claim 12 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and addresses on the recording medium.

14. The information recording/reproducing apparatus according to claim 11 wherein, as access positions described in said management information, positions where random accesses for said contents information are possible are extracted.

15. The information recording/reproducing apparatus according to claim 14 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

16. An information recording method comprising the steps of:

inputting contents information;

extracting access positions for said contents information inputted;

creating management information showing one or more access positions for said contents information; and

writing said contents information inputted and said management information on the recording medium.

17. The information recording method according to claim 16 wherein, said management information shows the access positions for contents information by means of the time information for the contents information and the addresses on the recording medium.

18. The information recording method according to claim 17 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps for said transport stream and the addresses on the recording medium.

19. The information recording method according to claim 16 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

20. The information recording method according to claim 19 wherein, said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are extracted.

21. An information reproducing method comprising the steps of:

reading contents information and management information from a recording medium on which said contents information and said management information showing one or more access positions for said contents information; and

controlling the reading positions of said contents information on said recording medium based on said management information read from said recording medium.

22. The information reproducing method according to claim 21 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

23. The information reproducing method according to claim 22 wherein, said contents information is recorded on a recording medium in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

24. The information reproducing method according to claim 21 wherein, as access positions described in said management information, positions where random accesses to said contents information are possible are shown.

25. The information reproducing method according to claim 24 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are indicated.

26. An information recording/reproducing method comprising the steps of:

during the recording process, inputting contents information, extracting the access positions for said contents information inputted, creating management information showing one or more access positions for said contents information, and writing said contents information inputted and said management information on the recording medium; and

during the reproducing process, reading said contents information and said management information from said recording medium, and controlling the reading positions of said contents information on said recording medium based on said management information read from said recording medium.

27. The information recording/reproducing method according to claim 26 wherein, said management information shows the access positions for contents information by means of the time information for the contents information and the addresses on the recording medium.

28. The information recording/reproducing method according to claim 27 wherein, said contents information is inputted in the form of transport streams prescribed by the

MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport stream and the addresses on the recording medium.

29. The information recording/reproducing method according to claim 26 wherein, as access positions described in said management information, positions where random accesses to said contents information are possible are extracted.

30. The information recording/reproducing method according to claim 29 wherein, said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are extracted.

31. A recording medium wherein,

contents information, and

management information extracted from said contents information and showing one or more access positions for this contents information are recorded.

32. An information recording apparatus comprising:

inputting means for inputting enciphered contents information;

contents information decoding means for decoding said enciphered contents information;

management information creating means for extracting the access positions for



said contents information from the contents information obtained by decoding enciphered contents information and for creating management information showing one or more access positions for said contents information; and

recording means for recording said enciphered contents information, information for enciphering said contents information as well as said created management information on a recording medium.

33. The information recording apparatus according to claim 32 further comprising:

receiving means for receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other apparatuses by means of communication means; and

cipher key enciphering means for creating enciphered cipher keys obtained by enciphering cipher keys received by said receiving means by the first cipher key, and wherein

said contents information decoding means uses the received cipher key to decode the enciphered contents information received to obtain contents information; and

said recording means records said enciphered cipher keys on said recording medium as information for enciphering said contents information.

34. The information recording apparatus according to claim 33 further comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher key by using recording medium identification information read from said

recording medium.

35. The information recording apparatus according to claim 33 further comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher key; and

second cipher key creating means for deciding the second cipher key used to encipher the first cipher key by using the recording medium identification information read from said recording medium.

36. The information recording apparatus according to claim 33 further comprising:

second cipher key creating means for deciding the second cipher key used to decode the first cipher key enciphered and read from said recording medium based on the recording medium identification information read from the said recording medium; and

the first cipher key decoding means for decoding the first cipher key enciphered by using said second cipher key created, wherein

said cipher key enciphering means enciphers the cipher keys received from said receiving means by using said first cipher key.

37. The information recording apparatus according to claim 32 further comprising:

receiving means for receiving enciphered contents information and the cipher keys used to encipher said contents information transmitted from other apparatuses by means of communication means;

cipher key creating information creating means for creating cipher key creating

information used to create cipher keys based on the cipher keys received from said receiving means; and

cipher key creating information creating means for creating enciphered cipher key creating information obtained by enciphering by the first cipher key said cipher key creating information created, and wherein

said contents information decoding means decodes the enciphered contents information received by means of cipher keys received to restore contents information; and wherein

said recording means records said enciphered cipher key creating information on said recording medium as information for enciphering said contents information.

38. The information recording apparatus according to claim 32 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

39. The information recording apparatus according to claim 38 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

40. The information recording apparatus according to claim 32 wherein, as access

positions described in said management information, positions where random accesses for said contents information are possible are extracted.

41. The information recording apparatus according to claim 40 wherein,

said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

42. An information reproducing apparatus comprising:

management information reading means for reading enciphered contents information, information for enciphering said contents information and management information from a recording medium in which said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded;

reading position controlling means for controlling the reading positions of said enciphered contents information on said recording medium and said information for enciphering said contents information; and

decoding means for decoding said enciphered contents information based on said information for enciphering said contents information.

43. The information recording apparatus according to claim 42 wherein, said recording medium contains an enciphered cipher key obtained by enciphering the

cipher key used for enciphering contents information as information for enciphering said contents information, and further comprising:

cipher key decoding means for decoding said enciphered cipher key by means of the first cipher key.

44. The information reproducing apparatus according to claim 43 further comprising:

first cipher key creating means for deciding the first cipher key used to decode said cipher key by said cipher key decoding means using the recording medium identification information read from said recording medium.

45. The information reproducing apparatus according to claim 43 further comprising:

first cipher key decoding means for decoding the first cipher key used to decode said cipher key using the second cipher key; and

second cipher key creating means for deciding the second cipher key used to decode said first cipher key by means of the recording medium identification information read from said recording medium.

46. The information reproducing apparatus according to claim 43 further comprising:

second cipher key creating means for deciding the second cipher key used to decode the first enciphered cipher key read from said recording medium based on the recording medium identification information read from said recording medium; and

first cipher key decoding means for decoding said first cipher key enciphered by means of said second cipher key created.

47. The information reproducing apparatus according to claim 42 wherein, said

recording medium contains enciphered cipher key creating information obtained by enciphering the cipher key creating information for creating the cipher keys used to encipher said contents information; and further comprising:

cipher key creating information decoding means for decoding said enciphered cipher key creating information by means of the first cipher key; and

cipher key creating means for creating said cipher key based on the cipher key creating information decoded by the first cipher key.

48. The information reproducing apparatus according to claim 42 wherein, said management information shows the access positions for contents information by means of the time information of the contents information and the addresses on the recording medium.

49. The information reproducing apparatus according to claim 48 wherein, said contents information is inputted by transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

50. The information reproducing apparatus according to claim 42 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

51. The information reproducing apparatus according to claim 50 wherein, said

contents information is inputted by transport streams prescribed by the MPEG 2 systems; and wherein

for access positions described in said management information, transport packets each containing a sequence header code are extracted.

52. An information recording/reproducing apparatus comprising:

inputting means for inputting enciphered contents information;

contents information decoding means for decoding said enciphered contents information;

management information creating means for extracting the access positions for contents information from said contents information decoded from said enciphered contents information and for creating management information showing one or more access positions for said contents information;

recording means for recording said enciphered contents information, information for enciphering said contents information, and said created management information on a recording medium;

management information reading means for reading enciphered contents information, said information for enciphering said contents information and said management information from said recording medium on which said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded;

a reading position controlling means for controlling the reading positions for said enciphered contents information on said recording medium and said information for enciphering said contents information based on the management information read from said recording medium; and

decoding means for decoding said enciphered contents information based on the information for enciphering said contents information.

53. The information recording/reproducing apparatus according to claim 52 further comprising:

receiving means for receiving enciphered contents information and the cipher keys used to encipher said contents information transmitted from other apparatuses by communication means;

cipher key enciphering means for creating enciphered cipher keys obtained by enciphering said cipher keys by means of the first cipher key; and

cipher key decoding means for decoding said enciphered cipher keys by means of the first cipher key, and wherein

said contents information decoding means decodes the enciphered contents information received by means of the cipher keys received to obtain contents information; and

said recording means records said enciphered cipher keys on said recording medium as information for enciphering said contents information.

54. The information recording/reproducing apparatus according to claim 53 further



comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher keys by means of the recording medium identification information read from said recording medium.

55. The information recording/reproducing apparatus according to claim 53 further comprising:

first cipher key creating means for deciding the first cipher key used to encipher said cipher keys;

first cipher key decoding means for decoding the first cipher key used to decode said cipher keys by means of the second cipher key; and

second cipher key creating means for deciding the second cipher key used to encipher said first cipher key by means of the recording medium identification information read from said recording medium.

56. The information recording/reproducing apparatus according to claim 53 further comprising:

second cipher key creating means for deciding the second cipher key for decoding the first cipher key enciphered and read from said recording medium based on the recording medium identification information read from the said recording medium; and

first cipher key decoding means enciphered by means of the second cipher key created, and wherein

said cipher key enciphering means decodes the cipher keys received by said receiving means by means of said first cipher key.

57. The information recording/reproducing apparatus according to claim 52 further comprising:

receiving means for receiving enciphered contents information and the cipher keys used to encipher said contents information transmitted from other apparatuses by communication means;

cipher key creating information creating means for creating cipher key creating information used to create such cipher keys;

cipher key creating information enciphering means for creating enciphered cipher key creating information obtained by enciphering said cipher key creating information created by the first cipher key, and wherein

said contents information decoding means decodes the enciphered contents information received by means of the cipher key received to restore contents information; and

said recording means records said enciphered cipher key creating information on said recording medium as information for enciphering said contents information.

58. The information recording/reproducing apparatus according to claim 52 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

59. The information recording/reproducing apparatus according to claim 58 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

60. The information recording/reproducing apparatus according to claim 52 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

61. The information recording/reproducing apparatus according to claim 60 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

62. An information recording method comprising the steps of:

inputting enciphered contents information;

decoding said enciphered contents information;

extracting the access positions for contents information from said contents information obtained by decoding the enciphered contents information;

creating management information showing one or more access positions for said contents information; and

recording said enciphered contents information, information for enciphering said contents information and said created management information on a recording medium.

63. The information recording method according to claim 62 further comprising the steps of:

receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods using communication means;

creating enciphered cipher keys obtained by enciphering the received cipher keys by means of the first cipher key;

decoding the received enciphered contents information using the received cipher keys to restore contents information; and

recording said enciphered cipher keys on said recording medium as information for enciphering said contents information.

64. The information recording method according to claim 63 further comprising the step of:

deciding the first cipher key used to encipher said cipher keys using the recording medium identification information read from said recording medium.

65. The information recording method according to claim 63 further comprising the steps of:

deciding the first cipher key used to encipher said cipher keys; and

deciding the second cipher key used to encipher said first cipher key using the

recording medium identification information read by said recording medium.

66. The information recording method according to claim 63 further comprising the steps of:

deciding the second cipher key used to encipher the first cipher key enciphered and read from said recording medium based on the recording medium identification information read from said recording medium;

decoding the first cipher key enciphered by means of said created second cipher key; and

enciphering the received cipher keys using said first cipher key.

67. The information recording/reproducing method according to claim 62 further comprising the steps of:

receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods using communication means;

creating cipher key creating information for creating these cipher keys based on the received cipher keys;

creating enciphered cipher key creating information obtained by enciphering by the first cipher key said created cipher key creating information;

decoding the enciphered contents information received using the cipher keys received to restore contents information; and

recording said enciphered cipher key creating information on said recording medium as information for enciphering said contents information.

68. The information recording method according to claim 62 wherein, said management information shows the access positions for contents information by means of the time information for contents information and addresses on the recording medium.

69. The information recording method according to claim 68 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport packets and addresses on the recording medium.

70. The information recording method according to claim 62 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

71. The information recording method according to claim 70 wherein, said contents information is inputted in the form of transport packets prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

72. An information reproducing method comprising the steps of:

reading enciphered contents information, information for enciphering said contents information and management information from a recording medium in which

said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded;

controlling the reading positions for said enciphered contents information on said recording medium and said information for enciphering said contents information based on the management information read from said recording medium; and

decoding said enciphered contents information is decoded based on the information for enciphering said contents information.

73. The information reproducing method according to claim 72 wherein, said recording medium contains enciphered cipher keys obtained by enciphering cipher keys used to encipher contents information; and further comprising the step of:

decoding said enciphered cipher keys by the first cipher key.

74. The information reproducing method according to claim 73 further comprising the step of:

deciding the first cipher key used to decode said cipher keys by means of the recording medium identification information read from said recording medium.

75. The information reproducing method according to claim 73 further comprising the steps of:

decoding the first cipher key used to decode said cipher keys by means of the second cipher key; and

deciding the second cipher key used to decode said first cipher key by means

of the recording medium identification information read from said recording medium.

76. The information reproducing method according to claim 73 further comprising the steps of:

deciding the second cipher key for decoding the enciphered first cipher key read from said recording medium based on the recording medium identification information read from said recording medium; and

decoding said enciphered first cipher key by means of said created second cipher key.

77. The information reproducing method according to claim 72 wherein, said recording medium contains enciphered cipher key creating information obtained by enciphering cipher key creating information for creating cipher keys used to encipher said contents information; further comprising the steps of:

decoding said enciphered cipher key creating information by means of the first cipher key; and

creating said cipher keys based on the cipher key creating information decoded by means of the first cipher key.

78. The information reproducing method according to claim 72 wherein, said management information shows the access positions for contents information by means of the time information for contents information and addressed on the recording medium.

79. The information reproducing method according to claim 78 wherein, said contents



information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and addresses on the recording medium.

80. The information reproducing method according to claim 72 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

81. The information reproducing method according to claim 80 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

82. An information recording/reproducing method comprising the steps of:

during the recording process, inputting enciphered contents information, decoding said enciphered contents information, extracting the access positions for contents information from said contents information obtained by decoding enciphered contents information, creating management information showing one or more access positions for said contents information, and recording said enciphered contents information and information for enciphering said contents information as well as said created management information on a recording medium; and

during the reproducing process, reading said enciphered contents information, said information for enciphering said contents information and said management information from a recording medium in which said enciphered contents information, said information for enciphering said contents information and said management information showing one or more access positions for said contents information are recorded; controlling the reading positions for said enciphered contents information on said recording medium and information for enciphering said contents information based on the management information read from said recording medium; and decoding said enciphered contents information based on information for enciphering said contents information.

83. An information recording/reproducing method according to claim 82 further comprising the steps of:

during the recording process, receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods by communication means, creating enciphered cipher keys obtained by enciphering received cipher keys by means of the first cipher key, decoding the enciphered contents information received by means of the received cipher keys to restore contents information and recording said enciphered cipher keys are recorded on said recording medium as information for enciphering said contents information; and

during the reproducing process, decoding said enciphered cipher keys by means of the first cipher key.

84. An information recording/reproducing method according to claim 83 further comprising the step of:

deciding the first cipher key used to encipher said cipher keys by means of the recording medium identification information read from said recording medium.

85. An information recording/reproducing method according to claim 83 further comprising the steps of:

deciding the first cipher key used to encipher said cipher keys; and

deciding the second cipher key used to encipher said first cipher key by means of the recording medium identification information read from said recording medium.

86. An information recording/reproducing method according to claim 83 further comprising the steps of:

deciding the second cipher key for decoding the first enciphered cipher key read from said recording medium based on the recording medium identification information read from said recording medium; and

decoding the first enciphered cipher key by means of said second cipher key created; and wherein

the cipher keys received are decoded by means of said first cipher key.

87. An information recording/reproducing method according to claim 82 further comprising the steps of:

during the recording process, receiving enciphered contents information and cipher keys used to encipher said contents information transmitted from other methods

by communication means, creating cipher key creating information for creating these cipher keys based on the cipher keys received, creating enciphered cipher key creating information obtained by enciphering said created cipher key creating information by means of the first cipher key, decoding the received enciphered contents information received by means of the cipher keys received to restore contents information, and recording said enciphered cipher key creating information on said recording medium as information for enciphering said contents information; and

during the reproducing process, decoding said enciphered cipher key creating information by means of the first cipher key, and creating said cipher keys based on the cipher key creating information decoded by the first cipher key.

88. An information recording/reproducing method according to claim 82 wherein, said management information shows the access positions for contents information by means of the time information for contents information and the addresses on the recording medium.

89. An information recording/reproducing method according to claim 88 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

90. An information recording/reproducing method according to claim 82 wherein, as

access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

91. An information recording/reproducing method according to claim 90 wherein, said contents information is inputted in the form of transport packets prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

92. A recording medium wherein,

enciphered contents information,

information for enciphering said contents information, and

management information extracted from said contents information and showing one or more access positions for said contents information are recorded.